State of West Virginia Office of Technology
Policy: Acceptable Use of State-Provided Wireless Devices
Issued by the CTO

1.0 PURPOSE **(Underlined terms are defined in Section 7.0 of document)**

This policy establishes guidelines for procurement, possession, and appropriate use of West Virginia state-owned and/or paid wireless communication equipment and/or service within the Executive Branch.

Wireless service includes, but may not be limited to the following: voice, data, text messaging, voicemail, caller ID, call waiting, call forwarding, and three-way calling.

2.0 SCOPE

This policy applies to all employees who utilize State-owned and/or State paid wireless communication equipment and/or services, and their immediate supervisors, as well as all wireless communication service contracts entered into by the State on behalf of employees, effective as of the date of this policy.

With the rapidly changing nature of electronic media, this policy cannot provide procedures to cover every possible situation. It expresses the State of West Virginia's philosophy and sets forth general principles to be applied to use of electronic media and services.

This policy will supersede all other previous wireless communication policies within the Executive Branch.

3.0 BACKGROUND

Under the provisions of West Virginia Code §5A-6-4a, the Chief Technology Officer (CTO) is granted both the authority and the responsibility to develop information

technology policy, promulgate that policy, audit for policy compliance, and require corrective action where compliance is found to be unsatisfactory or absent. The Governor's Executive Order No. 6-06, signed on August 16, 2006, empowers the CTO to "issue information security policies applicable to all Executive Branch department-level organizations." This policy is one in a series of Information Technology (IT) related policies intended to define and enable the incorporation of appropriate practices into all activities using technology in the State of West Virginia.

4.0 RELEVANT DOCUMENTS/MATERIAL

4.1 West Virginia Office of Technology

4.2 WVOT- IT Security Web Page

4.3 WVOT Policies Issued by the Chief Technology Officer (CTO)

4.4 West Virginia Code §5A-6-4a – "Duties of the Chief Technology Officer Relating to Security of Government Information"

5.0 RESPONSIBILITY/REQUIREMENTS

5.1 Conditions of Use

5.1.1 Each department is responsible for monitoring and controlling the wireless communication spending, and for keeping costs within its budget.

5.1.2 Wireless devices and service are to be used for State business when landline phone use is unavailable or impractical.

5.1.3 Occasional, limited, and appropriate personal use of wireless devices and services is allowed, but may be revoked at any time. (For more information, as well as examples of acceptable and unacceptable uses see "Cellular Phones and Other Wireless Devices" in Appendix A, Technology Usage Practices".)

5.1.4 Employees should have no expectation of privacy regarding their use of wireless devices. The State reserves the right to review calls, voicemail messages, text messages, etc., on all State-provided wireless devices.

5.1.4.1 The State will, consistent with applicable law and for any legitimate business reason, exercise its right to monitor, inspect, and/or review the contents of all State wireless devices at any time without the consent, presence, or knowledge of the affected employee. This may include usage, voicemail, text messages, and/or e-mail.

5.1.5 Employees will NOT be permitted to carry multiple State issued wireless communication devices if one will provide similar coverage and/or service, (ex: employees will not be able to have a Blackberry with integrated voice and data service as well as a wireless phone, or carry a pager in addition to a text message-enabled wireless phone if the geographic coverage is equivalent on both devices.)

5.1.6 Reasonable precautions should be taken to prevent equipment theft and/or vandalism. Employees must report lost or stolen wireless devices to a supervisor as soon as the loss becomes apparent.

5.2 Procurement

5.2.1 The State will negotiate services with several cellular providers via statewide contract(s). All cellular services must be acquired through the statewide contract(s).

5.2.1.1 Individual agencies will NOT be authorized to create separate contract(s) with cellular suppliers.

5.2.1.2 The State reserves the right to change service or plans at any time, for any reason, when it is in the best interest of the State.

5.2.1.3 Wireless equipment and/or services obtained independently from the statewide contract(s) will not be eligible for State reimbursement.

5.2.1.4 Wireless integrated devices, "SmartPhones" (i.e. Blackberry, Treo, and personal digital assistants [PDA] with both voice and data capabilities), or air [edge] cards are available through the statewide contract(s), and are subject to the same qualifying criteria as standard wireless devices.

5.2.1.4.1 Agency leadership approval is required for all new orders and/or reassignments of service based on established and objective needs criteria. (See Section 3.3)

5.2.2 Roles and Responsibilities

5.2.2.1 Supervisors will be responsible for the following:

5.2.2.1.1 Approving new service;

5.2.2.1.2 Terminating or reassigning service;

5.2.2.1.3 Recovering equipment or redistributing upon separation;

5.2.2.1.4 Tracking usage and spending; and

5.2.2.1.5 Adjusting service plans (as necessary) based on usage and spending;

5.2.2.2 Employees will be responsible for the following:

5.2.2.2.1 Responsible usage to minimize spending;

5.2.2.2.2 Recommending service plan adjustments based on increasing or decreasing usage requirements; and

5.2.2.2.3 Protection of equipment to prevent loss, unauthorized use, or disclosure of sensitive information.

5.2.2.3 The West Virginia Office of Technology (WVOT, working with the Department of Administration (DOA) Purchasing Division will be responsible for the following:

5.2.2.3.1 Negotiating contracts with suppliers; and

5.2.2.3.2 Regularly monitoring industry pricing and plan changes; and updating contracts to utilize improved plans and pricing.

5.3 Establishing a Need for Standard Wireless Service

5.3.1 Several criteria exist for establishing an approved need for standard wireless equipment and/or service (the more criteria that apply, the higher the need and likelihood of approval). This criterion includes, but may not be limited to the following:

5.3.1.1 A requirement to travel frequently on State-related business with a need beyond a calling card;

5.3.1.2 Large amounts of time spent away from the office without access to a landline;

5.3.1.3 A need for other state employees to be in constant communication with the individual;

5.3.1.4 A need for the individual to communicate frequently to support State business objectives while traveling; and/or

5.3.1.5 A consistent need for business communication outside normal business hours.

6.0 ENFORCEMENT

Any employee found to have violated this policy may be subject to disciplinary action up to and including dismissal. Disciplinary action, if determined to be necessary, will be administered by the employing Agency and may be based on recommendations of the WVOT and the West Virginia Division of Personnel, intended to address severity of the violation and the consistency of sanctions.

7.0 DEFINITIONS

7.1 Chief Technology Officer (CTO) – The person responsible for the State's information resources.

7.2 Contractor – Anyone who has a contract with the State or one of its entities.

7.3 Employee – Individuals retained and authorized on a temporary or permanent basis by the State of West Virginia to perform a service. For the purposes of Information Technology and Security policy, the term "employee" shall include the following: contractors, subcontractors, contractors' employees, volunteers, county health department staff, business associates, and any other persons who are determined and notified by the WVOT to be subject to this policy. This definition does not create any additional rights or duties.

7.4 Information Security Administrator (ISA) – The person designated by the agency head to assure the agency's compliance with State Information

Security policies and procedures. The ISA is the agency's internal and external point of contact for all Information Security matters.

7.5 Information Security Liaison (ISL) - Employees assigned by the ISA to assist in the protection of information resources.

7.6 Personal Digital Assistants (PDA) – A handheld device that combines computing, telephone/fax, and networking features. A typical PDA can function as a cellular phone, fax sender, and personal organizer.

7.7 Security Contact – These individuals include the ISL or the ISA.

7.8 SmartPhone – A wireless handheld device that supports e-mail, mobile telephone, text messaging, web browsing and other wireless information services. (ex: Blackberry, Treo, etc.)

7.9 West Virginia Division of Personnel – The Division of the Department of Administration established by WV CODE § 29-6-1 et seq., which is responsible for the system of human resource management for operating agencies in the classified and classified-exempt service of West Virginia State government.

7.10 West Virginia Office of Technology (WVOT) - The division of the Department of Administration established by WV Code § 5A-6-4a, et. seq., which is led by the State's CTO and designated to acquire, operate, and maintain the State's technology infrastructure. The WVOT is responsible for evaluating equipment and services, and reviewing information technology contracts.

7.11 Wireless Device – Any device that can communicate with other devices without being physically attached to them. Most wireless devices communicate through radio frequency.

8.0 LEGAL AUTHORITY (See West Virginia Code §5A-6-1 *et seq.*)

The CTO is charged with securing state government information and the data communications infrastructure from unauthorized uses, intrusions, or other security threats. The CTO has authority to issue policies, procedures, and standards to accomplish this mission. This policy will apply across the Executive Branch, with the exclusion of the West Virginia State Police, the Division of Homeland Security and Emergency Management, any constitutional officers, the West Virginia Board of Education, the West Virginia Department of Education, and the county boards of education. To the extent that there are policies in place which provide less security than this policy, they will be superseded by this policy. In instances where existing state and federal laws and regulations are more restrictive than IT policies issued by the WVOT the more restrictive provisions will prevail.

This policy is consistent with the following federal and state authorities:

- Omnibus Reconciliation Act of 1990, § 2201(c), 42 U.S.C. § 405(c)(2)(C)(viii)(I).
- Health Insurance Portability and Accountability Privacy Rule, 45 CFR 160 and 164
- Confidentiality of Substance Abuse Records, 42 U.S.C. 290dd-2; 42 CFR Part 2
- Gramm-Leach Bliley Act (GLBA), 15 U.S.C. § 6801, 16 CFR § 313
- Fair Credit Reporting Act, 15 U.S.C. § 1681 *et seq*.
- Driver's Privacy Protection Act, 18 U.S.C. § 2721
- Telemarketing Sales Rules, 16 CFR Part 310
- NIST SP 800-14 and NIST SP 800-53
- Executive Order No. 6-06 (August 16,2006)W. Va. Code § 5A-6-4a
- Freedom of Information Act, W. Va. Code § 29B-1-1 *et seq*.
- Records Management and Preservation of Essential Records Act, W. Va. Code §§ 5A-8-21, 22
- State Health Privacy Laws, **www.wvdhhr.org/hipaa/privacy**
- Confidentiality and Disclosure of Tax Returns and Return Information, W. Va. Code § 11-10-5d
- Uniform Motor Vehicle Records Disclosure Act, W. Va. Code 17A-2A-1 to14 WV Governmental Ethics Act, W. Va. Code § 6B-1-1 *et seq*.

9.0 INDEX

Acceptable/Unacceptable Use of State-provided Technology:

Computers, Email, Internet Access, and Wireless Devices

The information contained within this Appendix applies to the State of West Virginia Information Security policy and the Acceptable Use of State-Provided Wireless Devices policy.

Relevant Technologies

Include, but may not be limited to the following:

a. Personal computers;
b. Personal Digital Assistants (PDA);
c. Fax or copy machines with memory or hard drives;
d. Internet or Intranet;
e. E-mail;
f. Voice Mail;
g. Cell phones (including camera phones and smart phones with data communications and databases);
h. Pagers;
i. Media including disk drives, diskette drives, optical disks (CD), tape drives, and USB drives (flash drives);
j. Servers;
k. Printers

Unacceptable uses include, but are not limited to the following:

a. Any use which violates local, state, or federal laws;
b. Any use for commercial purposes, product advertisements, or "for-profit" **personal** activity;
c. Any use for viewing, transmitting, receiving, saving, or printing sexually explicit material;
d. Any use for promotion of political or religious positions or causes;
e. Any use in relation to copyright infringement;
f. Any use in relation to downloading, attaching, changing, distributing, or installing Any software or inappropriate files for non-business functions (ex: downloading MP3 files and/or broadcast audio or video files) including streaming content;
g. Any use in relation to participating in chain letters or unauthorized chat programs, or forwarding or responding to SPAM;

h. Any use for promoting harassment or illegal discrimination on the basis of race, gender, national origin, age, marital status, religion, or disability;
i. Any use for promoting the misuse of weapons or the use of devices associated with terrorist activities;
j. Any use related to pyramid selling schemes, multi-marketing schemes, or fundraising for any purpose unless agency sanctioned;
k. Any use for dispersing data to customers or clients without authorization;
l. Any use in relation to placing wagers or bets;
m. Any use that could be reasonably considered as disruptive to another's work;
n. Any sending or sharing of confidential information for unauthorized purposes;
o. Any personal use that can be construed as being other than minimal;
p. Any attachment or use of devices on the State network that are not owned by the State or authorized by the WVOT;
q. Redirecting State data to a non-State owned computing device or PDA on a routine basis, or without authorization from the CTO; or
r. Utilizing unauthorized peer-to-peer networking or peer-to-peer file sharing.

1. Employees will not waste IT resources by intentionally doing one or more of the following:
   a. Placing a program in an endless loop;
   b. Printing unnecessary amounts of paper;
   c. Disrupting the use or performance of State-provided IT resources or any other computer system or network; or
   d. Storing unauthorized information or software on State-provided IT resources.

2. Employees will not knowingly or inadvertently commit security violations. This includes doing one or more of the following:
   a. Accessing or attempting to access records within or outside the State's computer and communications facilities for which the employee is not authorized; or Bypassing State security and access control systems;
   b. Copying, disclosing, transferring, examining, re-naming, or changing information or programs belonging to another user unless given express permission to do so by the user responsible for the information or programs;
   c. Violating the privacy of individual users by reading e-mail or private communications without legal authority, or authorization based upon documented just cause;
   d. Misrepresenting oneself or the State of West Virginia;
   e. Making statements about warranty, express or implied, unless it is a part of normal job duties;
   f. Conducting any form of network monitoring, such as port scanning or packet filtering unless expressly authorized by the WVOT; or

g. Transmitting through the Internet confidential data, to include without limitation, credit card numbers, telephone calling cards numbers, logon passwords, and other parameters that can be used to access data without the use of encryption technology approved by the WVOT.

3. Employees will not commit security violations related to email activity. This includes doing one or more of the following:

   a. Sending unsolicited commercial email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material;
   b. Unauthorized use for forging of email header information;
   c. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies;
   d. Posting messages to large numbers of users (over 50) without authorization; or
   e. Posting from an Agency email address to newsgroups, blogs, or other locations without a disclaimer stating that the opinions expressed are strictly their own and not those of the State or the Agency, unless posting is in the fulfillment of business duties.

4. Employees will not knowingly or inadvertently spread computer viruses. To reduce this threat, employees must not import files from unknown or questionable sources.

Cellular Phones and other Wireless Devices

State-provided wireless devices are made available to any employee, who by the nature of their work, must be accessible at any time of day, day of the week, or from any location. The State has the right to monitor and review these devices for operational or management purposes.

1. Wireless Services include, but are not limited to, voice, data, text messaging, voicemail, caller ID, call waiting, call forwarding, and three-way calling.

2. Wireless devices are intended to provide the means for staff to conduct State business in environments when landlines or computer networks are not available. Personal use of wireless devices and service is prohibited except in certain limited and occasional circumstances that meet with the supervisor's approval. Personal use should only occur when it does not (1) interfere with the employee's work performance; (2) interfere with the work performance of others; (3) have undue impact on business operations; or (4) violate any other provision of this policy or any other State policy, procedure, or standard. Use of wireless devices is a privilege that may be revoked at any time. The State reserves the right to address excessive personal usage and recover the cost of excessive personal usage from the user. The following list should assist in setting a standard for **limited non-business use:**
   a. To alert household members about working late or other schedule changes;

b. To make alternative child care arrangements;
c. To talk with doctors, hospital staff, or day care providers;
d. To determine the safety of family or household members, particularly in an emergency;
e. To make funeral arrangements;
f. To reach businesses or other parties that can only be contacted during work hours; or
g. To arrange emergency repairs to vehicles or residences.

Unacceptable uses of State-provided wireless devices include, but may not be limited to the following:

1. Using the wireless device to make 900-number and toll calls;
2. Purchasing and downloading games, ring tones, and/or non-business related subscription services;
3. Using the wireless device while driving, without the use of a hands-free device, such as a headset, ear bud, or installation kit;
4. Using the wireless device to make directory assistance calls (Exceptions include emergency or unavoidable use);
5. Using the wireless device to call State toll-free numbers (State incurs double costs); and
6. Excessive personal use or personal use that causes additional charges on the invoice.

Employees must ensure that all non-business calls that cause incremental charges to the invoice are made at the employee's own expense, (e.g., charged to personal calling or credit cards, home telephones, or other non-State subsidized telephone numbers), and do not increase air time charges to the State.

Employee Responsibilities

Employees should conduct themselves as representatives of the State, and are responsible for becoming familiar with and abiding by all Information Security policies and guidelines.

1. Employees will only access files, data, and protected records if:
   a. The employee owns the information;
   b. The employee is authorized to receive the information; or
   c. The information is publicly available.

2. Employees are responsible for all activity that takes place through their userid. For example, employees must:
   a. Always use strong passwords; and
   b. NEVER share passwords with any individual for any reason.

Appendix A: Technology Usage Practices
State of West Virginia Office of Technology
Policy: Acceptable Use of State-Provided Wireless Devices

3. Employees must guard against access to files and take precautions to protect IT devices when away from the workstation. This includes but may not be limited to the following:
   a. Logging off computer;
   b. Locking computer; and/or
   c. Locking file cabinets and drawers

4. Employees are prohibited from monopolizing systems, overloading networks with excessive data, or wasting computer time, connect time, bandwidth, disk space, printer paper, or other IT resources.

5. Employees are prohibited from transmitting personal information about them or someone else without proper authorization while using State-provided IT resources.

6. Employees must report the following instances to a supervisor or designated security contact:

   a. Receiving or obtaining confidential information to which the employee is not entitled (Note: the owner or sender of such information must also be notified);
   b. Becoming aware of breaches in security; or
   c. Becoming aware of any inappropriate use of State-provided IT resource.

7. Employees must adhere to copyright law regarding the use of software, print or electronic information, and attributions of authorship. In certain instances, legal counsel can determine permissible uses.

Employees will contact an immediate supervisor if there is doubt concerning authorization to access any State-provided IT resource, or if questions arise regarding acceptable or unacceptable uses. If criminal activity is suspected or detected, reporting should occur up the supervisory or management chain without delay.

(WVOT) IT Policy Page)